Recomendaciones de Seguridad de 3Net Telecomunicaciones

Pornografía Infantil: Evite alojar, publicar o transmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se relacionen con actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquellas que la aclaren, modifiquen o adicionen, así como todas las leyes que lo prohíban.

Control de virus y códigos maliciosos: Siempre mantenga actualizado su antivirus en sus equipos y procuren correrlo periódicamente. Además, asegúrese de contar con elementos como anti-spyware y bloqueadores de ventanas emergentes. Evite visitar páginas no confiables o instalar software de procedencia dudosa. Es importante aplicar regularmente las actualizaciones en sistemas operativos y navegadores web, y deshabilitar características innecesarias como pop-ups, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas. En caso necesario, obtenga y configure un firewall personal para reducir el riesgo de exposición.

Correo electrónico: No publique su cuenta de correo en sitios no confiables y no preste su cuenta a terceros. Evite divulgar información confidencial o personal a través del correo y tenga precaución al recibir correos con advertencias sobre su cuenta bancaria. Nunca responda a correos HTML con formularios embebidos y cambie su contraseña inmediatamente si ingresa en un sitio no confiable.

Control de Spam y Hoax: No haga clic en enlaces dentro de correos electrónicos, incluso si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del navegador. Para asegurar la seguridad de los sitios, revise su certificado SSL. Evite reenviar correos de cadena para evitar congestiones en las redes y posibles robos de información.

Control de la Ingeniería Social: Evite divulgar información confidencial propia o de terceros y utilice los canales de comunicación adecuados para compartir información sensible.

Control de phishing y sus modalidades: No conteste correos, llamadas o mensajes de texto sospechosos sobre su cuenta bancaria. Valide con la entidad correspondiente la veracidad de los mensajes recibidos.

Robo de contraseñas: Cambie sus contraseñas frecuentemente, utilizando combinaciones fuertes de al menos 10 caracteres, números y caracteres especiales. Evite enviar información de claves a través de medios no encriptados.

Mecanismos de Seguridad

3Net Telecomunicaciones cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, así como protecciones para controlar el acceso a los servicios de Internet. Se han implementado configuraciones de seguridad base en los equipos de red y se establecen medidas de seguridad adicionales, incluyendo firewall, antivirus, antispam y filtrado de URLs para proteger tanto a los clientes como a la propia red de 3Net Telecomunicaciones. Los dispositivos de conexión final cuentan con elementos de autenticación y autorización para garantizar una conexión a Internet segura.